A much safer and easier way to make payments would be to own your own POS terminal which you could make all your transactions with. Unfortunately, a POS terminal is very expensive to purchase and to use since you have to pay a fee for each transaction, it is also too bulky to carry around with you, so in reality only a place of business can afford owning one.

A more practical solution would be if a credit card payment could be conducted using a well-known, non-bulky and commonly used device such as a mobile phone. However, an ordinary mobile phone does not have a built-in card reader where you could swipe your credit card, and even if that particular problem could be overcome, there is still an issue regarding the level of security a mobile phone provides. It is well known that for instance a spy program could infiltrate the mobile phone and hijack credit card information and identification information, such as the PIN code entered into the mobile phone via the mobile phone's keyboard when conducting a credit card payment, without the user even knowing about it.

In light of the above, a standard mobile phone is generally not considered to be a secure device, and thus not suitable for making credit card payments with. Thus, finding a way to make secure credit card payments with a mobile phone is highly sought after.

SUMMARY OF THE INVENTION

With the above description in mind, then, embodiments~~an aspect~~ of the present invention ~~is to~~ provide a way for any person or any company to easily and perform secure credit card payments which seek to mitigate, alleviate, or eliminate one or more of the above-identified deficiencies in the art and disadvantages singly or in any combination.

As will be described in more detail by the embodiment~~aspects~~ of the present invention below, one way for a private person or a company to easily and

securely perform secure credit card payments is to use a portable card reader device, a mobile phone communicating with a payment server, and a stand-alone secure PIN entry device, according to the aspects of the present invention below.

~~A first aspect of the present invention relates to a method of conducting electronic payments to a payment acquirer using a credit payment unit, comprising a smart card, card reader device, a mobile phone and a personal identification number (PIN) entry device, and a payment server, wherein said method comprising the steps of initializing said credit payment unit by establishing communication between said smart card and said card reader device, establishing communication between said card reader device and said mobile phone, and establishing communication between said mobile phone and said PIN entry device, establishing communication between said credit payment unit and said payment server using said mobile phone, communicating a reader serial number stored in said card reader device via said mobile phone to said payment server, communicating a PIN serial number stored in said PIN entry device to said payment server , deriving a reader key, used in said card reader device for encrypting information, in said payment server based on said communicated reader serial number and a master reader key stored in said payment server, deriving a PIN key, used in said PIN entry device for encrypting PIN information, in said payment server based on said communicated PIN serial number and a PIN master key stored in said payment server, reading, in said card reader device, smart card information from said smart card, and encrypting said smart card information using said reader key, receiving user inputted payment details and a user inputted signature in said mobile phone, receiving user inputted PIN information in said PIN entry device, encrypting said PIN information using said PIN key and communicating said encrypted PIN information to said payment server, communicating, using said mobile phone, said encrypted smart card information from said card reader device, said payment details, and said signature to said payment server, decrypting~~

~~and verifying said encrypted smart card information and said encrypted PIN information in said payment server, and communicating said payment details and said signature from said payment server to said payment acquirer server, and thereby completing an electronic payment.~~According to one aspect, there is provided a method of conducting electronic credit payments to a payment acquirer using a credit payment unit and a payment server, said credit payment unit comprising a smart card, a card reader device comprising electrical and physical interfaces required to fulfill EMV level 1 and a mobile phone, and said payment server comprising processing logic and data required to process a smart card application in order to perform an EMV transaction fulfilling EMV level 2, said method comprising: initializing said credit payment unit by establishing communication between said smart card and said card reader device, and establishing communication between said card reader device and said mobile phone and initiating a payment software in the mobile phone which begins setting up communication with the card reader device and also establishing communication over the internet with the payment server via a wireless or wired link; said card reader device communicating a reader serial number stored in said card reader device via said mobile phone to said payment server; said payment server deriving a reader key based on said communicated reader serial number and a master reader key stored in said payment server, said reader key being used in said card reader device and said payment server for encrypting all information exchanged between said card reader device and said payment server throughout the payment; said card reader device reading smart card information from said smart card, and encrypting said smart card information using said reader key; communicating, using said mobile phone, said encrypted smart card information from said card reader device to said payment server; decrypting and verifying said smart card information in said payment server; and only if the payment server has verified the smart card information, said mobile phone receiving user inputted payment details and a user inputted signature; communicating, using said mobile phone, said payment details and said signature to said payment server; and communicating said payment details from said payment server to said payment acquirer, and thereby completing an EMV compliant electronic credit payment.

The method may further comprise that the encrypted PIN information is communicated to said payment server via the mobile phone.

The method may further comprise that the encrypted PIN information is communicated wirelessly to said payment server.

The method may further comprise that the encrypted PIN information is communicated wirelessly to said payment acquirer server.

The method may further comprise that the decrypted encrypted PIN information is communicated from said payment server to said payment acquirer server for verification.

The method may further comprise that the communication between said credit payment unit and said payment server, using said mobile phone, is encrypted using the Transport Layer Security protocol or the Secure Sockets Layer protocol, and wherein said communication between said smart card and said card reader device is encrypted using said reader key in said card reader device.

The method may further comprise that the communicating of said payment details from said payment server to said payment acquirer server is encrypted.

The method may further comprise the steps of receiving, in said payment server, an acknowledgement from said payment acquirer server that said electronic credit payment has been completed, generating a receipt

of said electronic credit payment in said payment server, communicating said receipt to said credit payment unit, displaying said receipt in said mobile phone, and storing said receipt and said signature in a log.

The method may further comprise that the electronic credit payment complies with an EMV payment system specification.

Disclosed herein is~~A second aspect of the present invention relates to~~ a payment unit adapted to communicate with a payment server for making electronic payments, comprising, a smart card containing smart card information, a card reader device containing a unique reader serial number and a unique reader key, wherein said card reader device is adapted to read said smart card information and to encrypt said smart card information using said reader key, a PIN entry device containing a unique PIN serial number and a unique PIN key, wherein said PIN entry device is adapted to receive user inputted PIN information and encrypt said PIN information using said PIN key, and communicate said encrypted PIN information to said payment server, a mobile phone adapted to communicate with said payment server, wherein said mobile phone is further adapted to receive said reader serial number and said encrypted smart card information from said card reader device, wherein said mobile phone is further adapted to receive user inputted payment details and a user inputted signature, and wherein said mobile phone is further adapted to communicate said reader serial number, encrypted smart card information, payment details and signature to said payment server for completing a secure credit payment.

The payment unit may further comprise that said mobile phone is adapted to receive a receipt from said payment server and to display said receipt on a display in said mobile phone.

The payment unit may further comprise that said mobile phone is adapted to receive said inputted payment details via a touch sensitive display.

The payment unit may further comprise that said mobile phone is further adapted to receive said PIN serial number and said encrypted PIN information from said PIN entry device, and communicate said received PIN serial number and said encrypted PIN information to said payment server.

The payment unit may further comprise that said PIN entry device is adapted to communicate said PIN serial number and said encrypted PIN information to either said payment server or to a payment acquirer server.

~~A third aspect of the present invention relates to a system for conducting electronic credit payments to a payment acquirer using a credit payment unit according to claims 10 to 14, and wherein the system adapted to perform the method according to claims 1 to 9.~~According to another aspect, there is provided a system conducting electronic credit payments to a payment acquirer, said system comprising using a credit payment unit and a payment server, said credit payment unit adapted to communicate with said payment server for making electronic credit payments, said credit payment unit comprising a smart card, a card reader device and a mobile phone, wherein said smart card contains smart card information; wherein said card reader device contains a unique reader serial number, a unique reader key and electrical and physical interfaces required to fulfill EMV level 1, said reader key being used in said card reader device and said payment server for all information, exchanged between said card reader device and said payment server throughout the payment; wherein said payment server, has processing logic and data required to process a smart card application in order to perform an EMV transaction fulfilling EMV level 2, said payment server being adapted to derive a reader key based on said communicated reader serial number and a master reader key stored in said payment server, said reader key being used in said card reader device and said payment server for encrypting all information exchanged between said card reader device and said payment server throughout the payment and wherein said mobile phone adapted to: initialize said credit payment unit by

establishing communication between said smart card and said card reader device, and establishing communication between said card reader device and said mobile phone and initiating a payment software in the mobile phone which begins setting up communication with the card reader device and also establishing communication with the payment server over the internet via a wireless or wired link; communicate, said encrypted smart card information from said card reader device to said payment server; for decryption and verification of said smart card information in said payment server; and only if the payment server has verified the smart card information, said mobile phone receiving user inputted payment details and a user inputted signature; communicate, using said mobile phone, said payment details and said signature to said payment server; and wherein the payment server is further adapted to communicate said payment details from said payment server to said payment acquirer, and thereby completing an EMV compliant electronic credit payment.

BRIEF DESCRIPTION OF THE DRAWINGS

Further objects, features, and advantages of the present invention will appear from the following detailed description of some embodiments of the invention, wherein some embodiments of the invention will be described in more detail with reference to the accompanying drawings, in which:

Fig. 1a shows a smart card, a card reader device, a mobile phone and a stand-alone PIN entry device, constituting a secure payment unit, capable of making secure credit card payments; and

CLAIMS

1. A method of conducting EMV compliant electronic payments to a payment acquirer using a credit payment unit, comprising a smart card, card reader device comprising electrical and physical interfaces required to fulfil EMV level 1, a mobile phone and a personal identification number (PIN) entry device, and a payment server comprising processing logic and data required to process a smart card application in order to perform an EMV transaction fulfilling EMV level 2, wherein said method comprising:
    - initializing said credit payment unit by establishing communication between said smart card and said card reader device, establishing communication between said card reader device and said mobile phone, and establishing communication between said mobile phone and said PIN entry device and initiating a payment software in the mobile phone which begins setting up communication with the card reader device, the PIN entry device and also begins setting up communication over the internet with the payment server via a wireless or wired link;
    - communicating a reader serial number stored in said card reader device via said mobile phone to said payment server;
    - communicating a PIN serial number stored in said PIN entry device to said payment server;
    - deriving a reader key, used in said card reader device for encrypting information, in said payment server based on said communicated reader serial number and a master reader key stored in said payment server;
    - deriving a PIN key, used in said PIN entry device for encrypting PIN information, in said payment server based on said communicated PIN serial number and a PIN master key stored in said payment server;
    - said card reader device reading, smart card information from said smart card, and encrypting said smart card information using said reader key;
    - receiving user inputted payment details in said mobile phone;

- receiving user inputted PIN information in said PIN entry device, encrypting said PIN information using said PIN key and communicating said encrypted PIN information to said payment server;
- communicating, using said mobile phone, said encrypted smart card information from said card reader device, said payment details to said payment server;
- decrypting and verifying said encrypted smart card information and said encrypted PIN information in said payment server; and
- communicating said payment details from said payment server to said payment acquirer server, and thereby completing an electronic payment.

2. The method according to claim 1, wherein said encrypted PIN information is communicated to said payment server via the mobile phone.

3. The method according to claim 1, wherein said encrypted PIN information is communicated wirelessly to said payment server.

4. The method according to claim 1, wherein said encrypted PIN information is communicated wirelessly to said payment acquirer server.

5. The method according to any of claims 1 – 4, wherein said decrypted encrypted PIN information is communicated from said payment server to said payment acquirer server for verification.

6. The method according to any of claims 1 – 5, wherein said communication between said credit payment unit and said payment server, using said mobile phone, is encrypted using the Transport Layer Security protocol or the Secure Sockets Layer protocol, and wherein said communication between said smart card and said card reader device is encrypted using said reader key in said card reader device.

7. The method according to any of claims 1 - 6, wherein said communicating of said payment details from said payment server to said payment acquirer server is encrypted.

8. The method according to any of claims 1 – 7, further comprise:
   - receiving, in said payment server, an acknowledgement from said payment acquirer server that said electronic credit payment has been completed;
   - generating a receipt of said electronic credit payment in said payment server;
   - communicating said receipt to said credit payment unit;
   - displaying said receipt in said mobile phone; and
   - storing said receipt in a log.

9. A payment unit adapted to communicate with a payment server for making electronic payments, the payment server comprising processing logic and data required to process a smart card application in order to perform an EMV transaction fulfilling EMV level 2, the payment unit comprising:
   - a smart card containing smart card information;
   - a card reader device comprising electrical and physical interfaces required to fulfil EMV level 1, wherein the a card reader device contains a unique reader serial number and a unique reader key, wherein said card reader device is adapted to read said smart card information and to encrypt said smart card information using said reader key;
   - a PIN entry device containing a unique PIN serial number and a unique PIN key, wherein said PIN entry device is adapted to receive user inputted PIN information and encrypt said PIN information using said PIN key, and communicate said encrypted PIN information to said payment server;
   - a mobile phone adapted to initiate a payment software in the mobile phone which begins setting up the communication with the card reader device, the PIN entry device and also begins setting up

communication over the internet with a payment server via a wireless or wired link, wherein said mobile phone is further adapted to receive said reader serial number and said encrypted smart card information from said card reader device, wherein said mobile phone is further adapted to receive user inputted payment details, and wherein said mobile phone is further adapted to communicate said reader serial number, encrypted smart card information, payment details to said payment server to verify the smartcard information in the payment server fulfilling EMV Level 2 security measures for completing a secure credit payment in the payment server.

10. The payment unit according to claim 9, wherein said mobile phone is adapted to receive a receipt from said payment server and to display said receipt on a display in said mobile phone.

11. The payment unit according to any of claims 9 - 10, wherein said mobile phone is adapted to receive said inputted payment details via a touch sensitive display.

12. The payment unit according to any of claims 9 - 11, wherein said mobile phone is further adapted to receive said PIN serial number and said encrypted PIN information from said PIN entry device, and communicate said received PIN serial number and said encrypted PIN information to said payment server.

13. The payment unit according to any of claims 9 - 11, wherein said PIN entry device is adapted to communicate said PIN serial number and said encrypted PIN information to either said payment server or to a payment acquirer server.

14. A system for conducting electronic credit payments to a payment acquirer using a credit payment unit according to claims 9 to 13, and wherein the system adapted to perform the method according to claims 1 to 8.

CLAIMS:

1. A method of conducting electronic credit payments to a payment acquirer using a credit payment unit (100, 201) and a payment server (208), said credit payment unit comprising a smart card (108, 203), a card reader device (106, 202) comprising electrical and physical interfaces required to fulfill EMV level 1 and a mobile phone (101, 204), and said payment server comprising processing logic and data required to process a smart card application in order to perform an EMV transaction fulfilling EMV level 2, said method comprising:

- initializing said credit payment unit by establishing communication between said smart card and said card reader device, and establishing communication between said card reader device and said mobile phone and initiating a payment software in the mobile phone which begins setting up communication with the card reader device and also establishing communication over the internet with the payment server via a wireless or wired link;

- said card reader device communicating a reader serial number stored in said card reader device via said mobile phone to said payment server;

- said payment server deriving a reader key based on said communicated reader serial number and a master reader key stored in said payment server, said reader key being used in said card reader device and said payment server for encrypting all information exchanged between said card reader device and said payment server throughout the payment;

- said card reader device reading smart card information from said smart card, and encrypting said smart card information using said reader key;

- communicating, using said mobile phone, said encrypted smart card information from said card reader device to said payment server;

- decrypting and verifying said smart card information in said payment server; and only if the payment server has verified the smart card information, said mobile phone receiving user inputted payment details and a user inputted signature;

- communicating, using said mobile phone, said payment details and said signature to said payment server; and

- communicating said payment details from said payment server to said payment acquirer, and thereby completing an EMV compliant electronic credit payment.

2. The method according to claim 1, wherein said communication between said smart card and said card reader device is encrypted using said reader key in said card reader device.

3. The method according to any of claims 1 - 2, wherein said communication between said credit payment unit and said payment server using said mobile phone is encrypted using the Transport Layer Security protocol or the Secure Sockets Layer protocol.

4. The method according to any of claims 1 - 3, wherein said user inputted signature is a graphical image of said user's signature entered on a display on said mobile phone.

5. The method according to any of claims 1 - 4, wherein said communicating of said payment details from said payment server to said payment acquirer is encrypted.

6. The method according to any of claims 1 - 5, further comprising:

- receiving, in said payment server, an acknowledgement from said payment acquirer that said electronic credit payment has been completed.

7. The method according to any of claims 1 - 6, further comprising:

- generating a receipt of said electronic credit payment in said payment server;
- communicating said receipt to said credit payment unit; and
- displaying said receipt in said mobile phone.

8. The method according to claim 7, further comprising:

- storing said receipt and said signature in a log.

9. A system conducting electronic credit payments to a payment acquirer, said system comprising using a credit payment unit and a payment server, said credit payment unit adapted to communicate with said payment server for making electronic

credit payments, said credit payment unit comprising a smart card (108, 203), a card reader device (106, 202) and a mobile phone (101,204),

- wherein said smart card contains smart card information;

- wherein said card reader device contains a unique reader serial number, a unique reader key and electrical and physical interfaces required to fulfill EMV level 1, said reader key being used in said card reader device and said payment server for all information, exchanged between said card reader device and said payment server throughout the payment;

- wherein said payment server, has processing logic and data required to process a smart card application in order to perform an EMV transaction fulfilling EMV level 2, said payment server being adapted to derive a reader key based on said communicated reader serial number and a master reader key stored in said payment server, said reader key being used in said card reader device and said payment server for encrypting all information exchanged between said card reader device and said payment server throughout the payment and

- wherein said mobile phone adapted to:

- initialize said credit payment unit by establishing communication between said smart card and said card reader device, and establishing communication (304) between said card reader device and said mobile phone and initiating a payment software (310) in the mobile phone which begins setting up communication with the card reader device and also establishing communication (312) with the payment server over the internet via a wireless or wired link;

- communicate, said encrypted smart card information from said card reader device to said payment server; for decryption and verification of said smart card information in said payment server; and only if the payment server has verified the smart card information, said mobile phone receiving user inputted payment details (408) and a user inputted signature (412);

- communicate, using said mobile phone (414), said payment details and said signature to said payment server; and wherein the payment server is further adapted to communicate said payment details from said payment server to said payment acquirer, and thereby completing an EMV compliant electronic credit payment.

10. The credit payment unit according to claim 9, wherein said mobile phone is adapted to receive a receipt from said payment server and to display said receipt a display in said mobile phone.

11. The credit payment unit according to any of claims 9 - 10, wherein said mobile phone is adapted to receive said inputted payment details via a touch sensitive display.